Exec-SearchPath-02

Non-pathsearching Exec functions that run both .com and .exe files can be fooled into running malicious programs

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5738 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Indeterminate File/Path • Process management • Unconditional
Software Context	• Process Management
Location	
Description	Non-pathsearching Exec functions that run both .com and .exe files can be fooled into running malicious programs. Any function that executes an arbitrary command poses high risk for the application and should be carefully scrutinized. In this case, these functions will execute a .com program before a .exe program unless the file extension is fully specified. A call to one of the below mentioned functions should be flagged. Determine whether the extension is fully specified. The following functions do not search the path, but will run .com programs before .exe programs. Always specify the file extension with these APIs:
APIs	**FunctionName** / **Comments** _execl _execle _execv _execve _spawnl _spawnle _spawnv

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

_spawnve	
_texecl	
_texecle	
_texecv	
_texecve	
_tspawnl	
_tspawnle	
_tspawnv	
_tspawnve	
_wexecl	
_wexecle	
_wexecv	
_wexecve	
_wspawnl	
_wspawnle	
_wspawnv	
_wspawnve	

Method of Attack

These functions do not search the path, but will execute .com before .exe programs. Therefore, make sure you fully specify the extension to prevent file spoofing. This could allow an attacker to place a malicious .com program in the same location as a similar .exe program.

Exception Criteria

Solutions

Solution Applicability	Solution Description	Solution Efficacy
Whenever one of the indicated non-path-searching APIs is used.	When using these functions always include the file extension (.exe, .com, .bat) to prevent unwanted searches.	Effective.

Signature Details	Any of the indicated APIs, with no explicit file name extension.
Examples of Incorrect Code	`_execl("C:\\MyApp\\MyProgram", NULL); /* Note missing file extension */`
Examples of Corrected Code	`_execl("C:\\MyApp\\MyProgram.exe", NULL); /* Note inclusion of file extension */`
Source References	• Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, pg. 322 • man pages for execlp, execvp, popen, and system, Microsoft Developer Network Library. • Microsoft Developer Network Library
Recommended Resources	
Discriminant Set	**Operating Systems**: • Windows (All) • UNIX (All) **Language**:

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com